The GHZ/W-calculus contains rational arithmetic

Bob Coecke,* Aleks Kissinger,† Alex Merry‡
Oxford University Computing Laboratory, Quantum Group
Wolfson Building, Parks Road, Oxford OX1 3QD, UK
coecke/alek/alemer@comlab.ox.ac.uk

Shibdas Roy§
Center for Quant. Inf. and Quant. Comp.
Department of Physics, IISc, Bangalore
roy_shibdas@yahoo.co.in

Graphical calculi for representing interacting quantum systems serve a number of purposes: compositionally, intuitive graphical reasoning, and a logical underpinning for automation. The power of these calculi stems from the fact that they embody generalized symmetries of the structure of quantum operations, which, for example, stretch well beyond the Choi-Jamiolkowski isomorphism. One such calculus takes the GHZ and W states as its basic generators. Here we show that this language allows one to encode standard rational calculus, with the GHZ state as multiplication, the W state as addition, the Pauli X gate as multiplicative inversion, and the Pauli Z gate as additive inversion.

1 Introduction

Categorical quantum mechanics [1] aims to recast quantum mechanical notions in terms of symmetric monoidal categories with additional structure. One layer of extra structure, compactness [17], encompasses the well-known Choi-Jamiolkowski isomorphism. Compactness is itself subsumed by the much richer commutative Frobenius algebra structure [3], which governs classical data, observables, and certain tripartite states [8, 5, 6, 7]. In this symmetric monoidal form, quantum mechanics enjoys:

- an *operational interpretation* by making sequential and parallel composition of systems and processes the basic connectives of the language [4];
- an intuitive *diagrammatic calculus* [4] via the Penrose-Joyal-Street diagrammatic calculus for symmetric monoidal categories [19, 16], augmented with Kelly and Laplaza's coherence result for compact categories, and Lack's work on distributive laws [18];
- a *logical underpinning* [12] via the closed structure resulting from compactness.

The last allows the application of automated reasoning techniques to quantum mechanics [9, 10, 11]. A prototype software implementation, `quantomatic`, already exists and is jointly developed in Edinburgh and Oxford.

Categorical quantum mechanics has meanwhile been successful in solving problems in quantum information [13] and quantum foundations [6], where other methods and structures failed to be adequate. Key to these results is the description of *interacting basis structures* in [5]. The language of that paper consists of a pair of abstract bases or *basis structures*, which are, again in abstract terms, mutually unbiased, and an abstract generalisation of phases relative to bases. This formalism has been implemented in `quantomatic`, and is expressive enough to universally model any linear map $f : \mathbb{Q}^{\otimes n} \to \mathbb{Q}^{\otimes m}$, where

*Supported by EPSRC Advanced Research Fellowship EP/D072786/1, Office of Naval Research Grant N00014-09-1-0248 and EC FP6 STREP QICS. Some of this work was performed during a visit at IQOQI Vienna.

†Supported by a Clarendon scholarship

‡Supported by a DTA scholarship

§Funded by DST, Govt. of India

F. Ablayev, B. Coecke, A. Vasiliev (Eds.):
Workshop on High Productivity Computations (HPC 2010).
EPTCS 52, 2011, pp. 34–48, doi:10.4204/EPTCS.52.4

$\mathbb{Q} = \mathbb{C}^2$. On the other hand, if we restrict the language to the two basis structures only it becomes very poor, describing no more than 2 qubit states.

This brings us to the subject of this paper. In [7] two of the authors introduced pairs of interacting commutative Frobenius algebras that do not model bases, but the tripartite GHZ and W states [14]. Both these states can indeed be endowed with the structure of a commutative Frobenius algebra, yielding a *GHZ structure* and a *W structure* as we recall in Section 2. The main point of this paper is that the language consisting of the GHZ structure (which is essentially the same as a basis structure) and the W structure is already rich enough to encode rational arithmetic, with the exception of additive inverses. Now an infinite number of qubit states can be described, corresponding to the rational numbers of the arithmetic system. We demonstrate this in Section 3. In Section 4 we extend the GHZ/W-calculus with one basic graphical element which then allows additive inverses to be captured. Section 5 addresses the issue of how to implement the calculus within the `quantomatic` software.

We assume that the reader is familiar with the diagrammatic calculus for symmetric monoidal categories [16, 20], which is also reviewed in [7]. We also assume that the reader is familiar with the (very) basics of finite dimensional Hilbert spaces and Dirac notation as used in quantum computing.

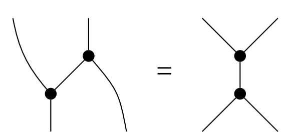
2 Frobenius Algebras and the GHZ/W-calculus

Fix a symmetric monoidal category $(\mathbf{V}, \otimes, I, \sigma)$. Throughout this paper, we shall define morphisms in $\mathbf{V}$ using the graphical notation defined in [20]. In this notation, 'wires' correspond to objects and vertices, and 'boxes' correspond to morphisms. We shall express composition vertically, from top to bottom, and the monoidal product as (horizontal) juxtaposition of graphs. When wires are not labeled, they are assumed to represent a fixed object, Q.

Example 2.1. A canonical example throughout will be **FHilb**, the category of finite-dimensional Hilbert spaces and linear maps. In this case, $\otimes$ is the usual tensor product, σ the swap map $v \otimes w \mapsto w \otimes v$, $I := \mathbb{C}$ and $Q := \mathbb{C}^2$, the space of qubits. We shall also refer the "projective" category of finite-dimensional Hilbert spaces, $\mathbf{FHilb}_p$, whose objects are the same as **FHilb** and whose arrows are linear maps, taken to be equivalent iff they differ only by a non-zero scalar.

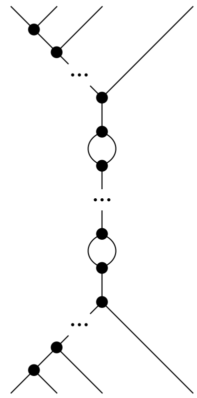
2.1 Commutative Frobenius Algebras

A *commutative Frobenius algebra* (CFA) consists of an internal commutative monoid $(Q, \ , \ )$ and an internal cocommutative comonoid $(Q, \ , \ )$ that interact via the Frobenius law:

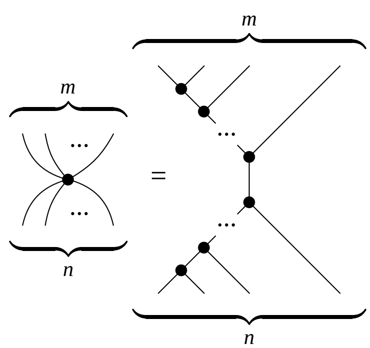


One can show that any connected graph consisting only of , , , , σ and 1_Q depends only upon

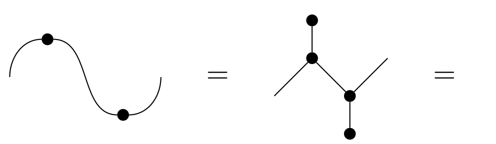
the number of inputs, outputs, and loops. As such, it can be reduced to a canonical normal form:



In any connected graph, loops are counted as the total number of edges that can be removed without disconnecting the graph. We shall use ‘spider’ notation to represent graphs of Frobenius algebras using vertices of any arity. We express any connected graph as above with m inputs, n outputs, and no loops as a single vertex of the same colour:

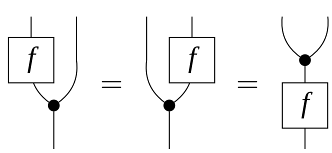


We give two of these graphs special names. The *cup* is defined as  and the *cap* is defined as . These induce a compact structure, since



2.2 Phases

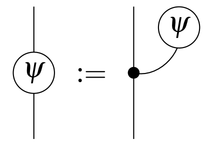
Definition 2.2. [5] Given a CFA on an object A, a morphism $f : A \to A$ is a *phase* if we have



(1)

Equivalently, phases can be described as module endomorphisms, where  is considered as a left (or right) module over itself.

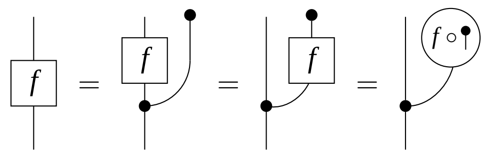
Proposition 2.3. *A phase $f : A \to A$ can be equivalently defined as a morphism of the form:*



(2)

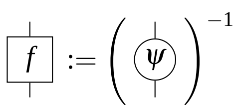
for some element $\psi : \mathrm{I} \to A$.

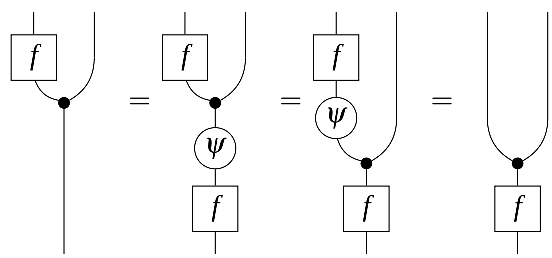
Proof. Given eqs. (1) we have



where we used unitality of the CFA, and conversely, given eq. (2), eqs. (1) straightforwardly follow by associativity and commutativity of the CFA. □

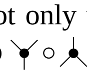
Proposition 2.4. *The inverse of a phase is a phase.*

Proof. Setting  we have

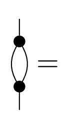


□

2.3 GHZ/W calculus

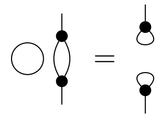
In this paper, we are concerned not only with general CFAs, but two specific cases, depending on the behaviour of the loops. We refer to  as the *loop map* of a CFA.

Definition 2.5. [7] A *GHZ-structure* is a special commutative Frobenius algebra; that is, a commutative Frobenius algebra where the loop map is equal to the identity:



These GHZ-structures have also been referred to as *basis structures*, for example in [6], because of their strong connection to bases in finite-dimensional vector spaces. See Theorem 2.10 below.

Definition 2.6. [7] A *W-structure* is an anti-special commutative Frobenius algebra. This is commutative Frobenius algebra whose loop map obeys the following equation:

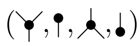
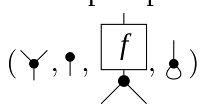


(3)

where we use the following short-hand notation:

This distinction essentially comes down to whether the loop map is singular or invertible.

Lemma 2.7. *If the loop map of a CFA is an isomorphism, the CFA can be made special via a phase.*

Proof. Consider a CFA . Since its loop map is a phase, by Proposition 2.4 so is the inverse of the loop map, which we denote f. Then  is easily seen to be a special CFA. □

Lemma 2.8 (Herrmann [15])**.** *If the loop of a CFA is disconnected, i.e. factors over the tensor unit, then it obeys eq.* (3)*, that is the CFA is necessarily anti-special.*

The following is an example of a GHZ-structure in **FHilb**:

 $= |0\rangle\langle 00| + |1\rangle\langle 11|$  $= \sqrt{2}|+\rangle := |0\rangle + |1\rangle$

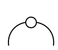
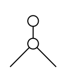
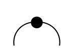
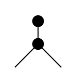
 $= |00\rangle\langle 0| + |11\rangle\langle 1|$  $= \sqrt{2}\langle +| := \langle 0| + \langle 1|$ (4)

and we also have an example of a W-structure in **FHilb**:

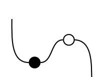
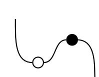
 $= |1\rangle\langle 11| + |0\rangle\langle 01| + |0\rangle\langle 10|$  $= |1\rangle$

 $= |00\rangle\langle 0| + |01\rangle\langle 1| + |10\rangle\langle 1|$  $= \langle 0|$ (5)

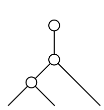
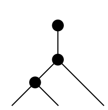
Note that the cups for these CFAs do not coincide:

 $:=$  $= |00\rangle + |11\rangle$  $:=$  $= |01\rangle + |10\rangle$

However, the composition of a cap from one CFA with a cup from the other yields the Pauli X, or 'NOT', gate:

 $:=$  $=$  $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

These CFAs respectively induce the following tripartite states:

 $= |000\rangle + |111\rangle = |GHZ\rangle$  $= |100\rangle + |010\rangle + |001\rangle = |W\rangle$

As the name suggests, the associated tripartite state of the above GHZ-structure is a GHZ state, and that of the W-structure is a W state. Furthermore, Theorem 2.9 asserts that for qubits, the associated tripartite state of *any* GHZ-structure (resp. W-structure) is a GHZ state (resp. W state), up to local operations.

Theorem 2.9. [7] *For any special (respectively anti-special) CFA on a qubit in* **FHilb**, *the induced tripartite state is SLOCC-equivalent to* $|GHZ\rangle$ *(respectively* $|W\rangle$*). Furthermore, any tripartite state* $|\Psi\rangle$ *either induces a special or anti-special CFA-structure, depending on whether it is SLOCC-equivalent to* $|GHZ\rangle$ *or to* $|W\rangle$.

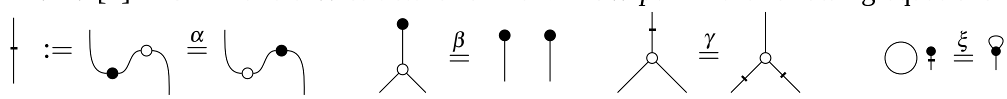
Theorem 2.10 justifies the alternative name *basis structure* for GHZ-structures.

Theorem 2.10. [2] *Special commutative Frobenius algebras on a finite-dimensional Hilbert space* $\mathscr{H}$ *are in 1-to-1 correspondence with (possibly non-orthogonal) bases for* $\mathscr{H}$.

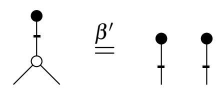
For any special CFA, phases are matrices that are diagonal in the corresponding basis. The corresponding $|\psi\rangle$ (as in proposition 2.3) lies on the equator of the Bloch sphere, justifying the name 'phases'.

We can also consider interactions between a GHZ-structure and a W-structure.

Definition 2.11. [7] A GHZ- and a W-structure form a *GHZ/W-pair* if the following equations hold:



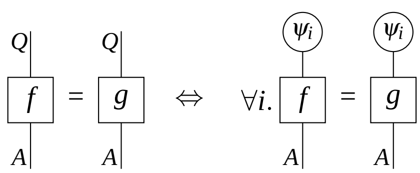
By eqs. (β, γ) we also have:



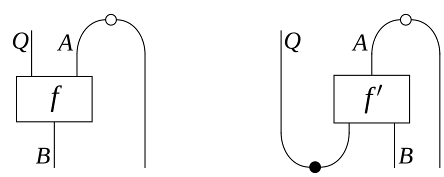
2.4 Plugging

Since we are often concerned with objects in a monoidal category that are finitary in nature, we can deduce many new identities using a technique we call *plugging*.

Definition 2.12. A set of points $\{\psi_i : I \to Q\}$ form a *plugging set* for Q if they suffice to distinguish maps from Q. That is, for all objects A and maps $f, g : Q \to A$,



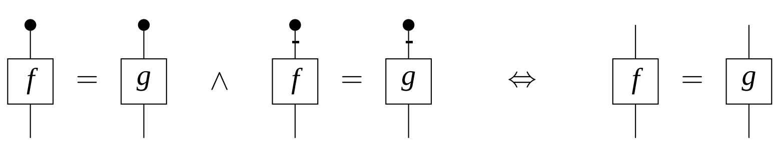
When we prove a graphical identity by showing two maps are not distinguished by a plugging set, we call this 'proof by plugging.' Also note that we can extend such proofs to maps of the form $f : Q \otimes A \to B$ or $f' : A \to Q \otimes B$ by using the Frobenius caps and cups when Q has a CFA (, , ,) and A a CFA (, , ,),



The axioms of a GHZ/W-pair suffice to prove the following lemma for Hilbert spaces.

Lemma 2.13 ([7])**.** *For a GHZ/W-pair on H in* **FHilb** *with* $\dim(H) \geq 2$, *the points and span a 2-dimensional space; hence for* $H = \mathbb{C}^2$ *the points and form a basis.*

Motivated by this fact, we assume the that { , } forms a plugging set for Q. More explicitly:



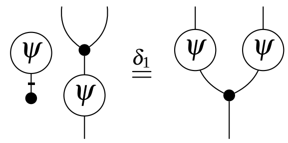
3 Arithmetic from a GHZ/W-pair

Given a GHZ/W-pair, we can extract an arithmetic system. First, we establish some preliminary results.

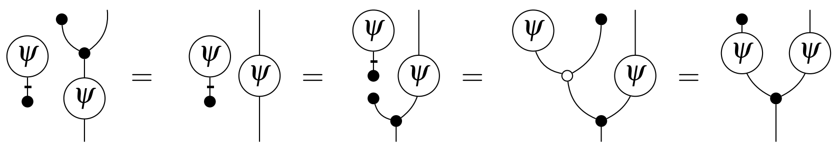
3.1 Properties of GHZ-phases

Below, all phases are GHZ-phases. When relying on plugging, we have the following:

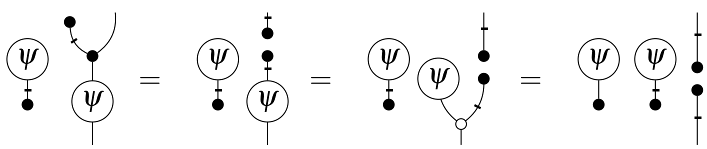
Theorem 3.1.

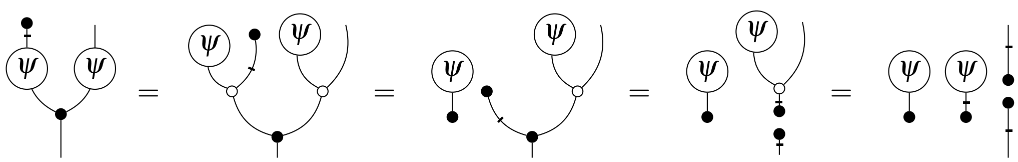


Proof. Plugging to one input:



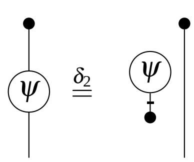
Plugging to one input of both sides:



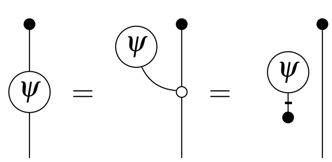


□

Theorem 3.2.

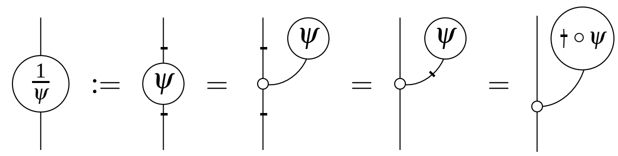


Proof.



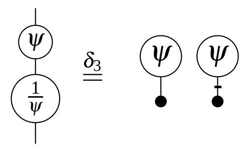
□

Note that for -phases we have:

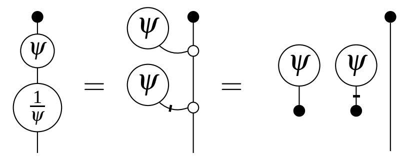


The particular choice of notation $\frac{1}{\psi}$ is justified below, and will play a key role in this paper.

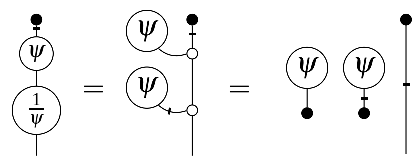
Theorem 3.3.



Proof. Plugging into the input:

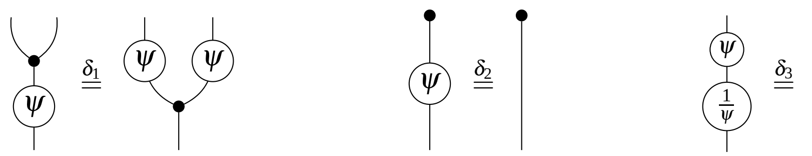


Plugging into the input:



□

In a setting like $\mathbf{FHilb}_p$, where we ignore cancelable scalar multipliers, and provided that the scalars and in the equation are cancelable, eqs. (δ_1, δ_2, δ_3) simplify to:



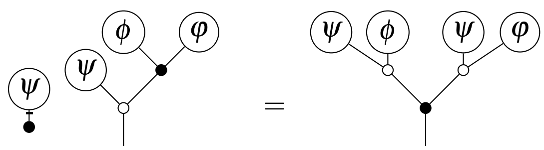
Examples of phases for which some of these simplified equations fail to hold are:

3.2 Natural Number Arithmetic

Assume that we are given a GHZ/W-pair. In particular, we have two internal commutative monoids (,) and (,). We will now consider the induced commutative monoids on elements:

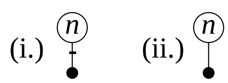
We will call applied to elements *addition* and applied to elements *multiplication*, for reasons that will become apparent shortly. Similarly, we call the *unit for addition* and the *unit for multiplication*. By Theorem 3.1 we have a distributivity law, up to a scalar, partially explaining our choices of the names addition and multiplication for the monoids:

Corollary 3.4.

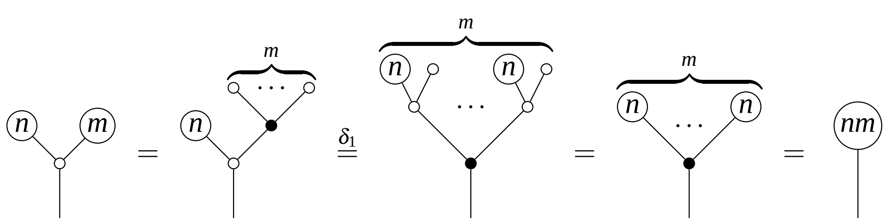


Moreover, we can use these to do concrete arithmetic on the natural numbers. We start by defining an encoding for the natural numbers:

From hence forth, we shall assume we are working in a category with no non-trivial invertible (i.e. non-zero) scalars, such as $\mathbf{FHilb}_p$. Thus, we shall drop any invertible scalars. Furthermore, we shall assume scalar (i.) is invertible for all n and scalar (ii.) is invertible for all $n \neq 0$:



That is the normal addition operation for these numbers follows immediately from their definition and associativity of . We can also show that is the normal multiplication operation (noting first that the encoding of 1 is , and hence the unit of):

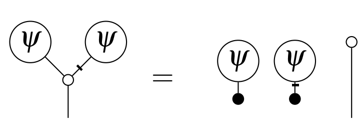


The distributivity law stated earlier now translates into the normal distributivity of multiplication over addition in the natural numbers, up to a scalar.

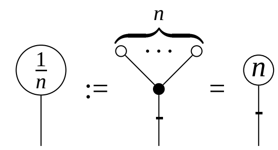
3.3 Multiplicative inverses

By Theorem 3.3 we have that is also an inverse for , up to a scalar:

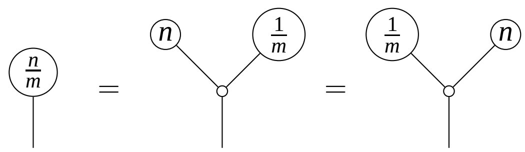
Corollary 3.5.



Hence, we have an encoding for the multiplicative inverses of the natural numbers:

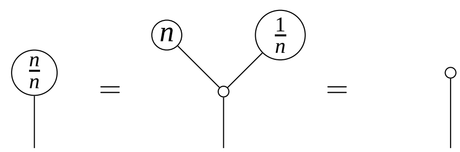


Thoughtout this paper, we shall assume any natural number occurring in the denominator is not equal to 0. This allows us to encode positive fractions in the following form:



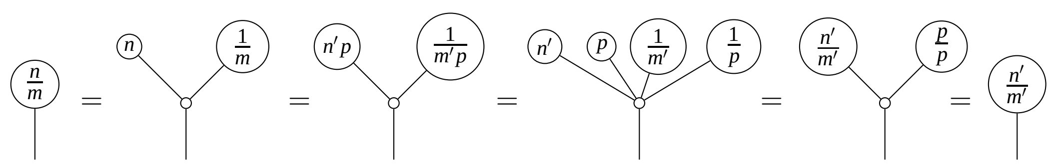
where the second equality follows from associativity and commutativity of the GHZ-structure.

Remark 3.6. It should be noted that the construction of this encoding depends on the choice of numerator and denominator, and not just on the rational number being represented. Therefore, we should demonstrate that the actual point depends only on the number represented. We start by noting that, by corollary 3.5,

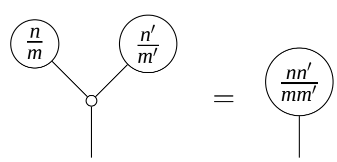


where we have ignored the scalar in corollary 3.5, since it is cancellable for the points that we have used to encode the natural numbers.

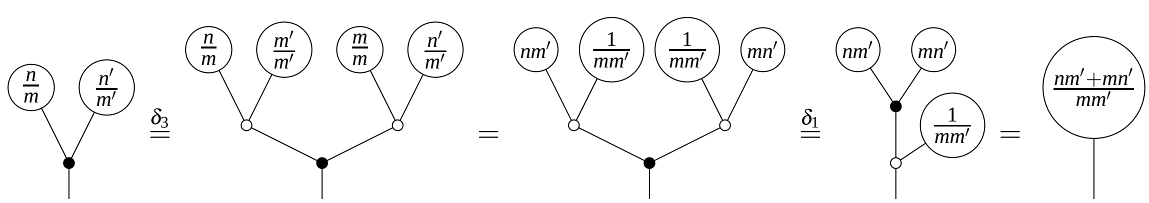
We know that if $\frac{n}{m} = \frac{n'}{m'}$, there is a p such that $n = n'p$ and $m = m'p$, so it follows easily that



Example 3.7. All the usual properties of fractions follow in a straightforward manner from the axioms of rational arithmetic that we have proved. For example,



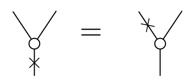
is immediate from the associativity commutativity of the GHZ-structure, and we also have:



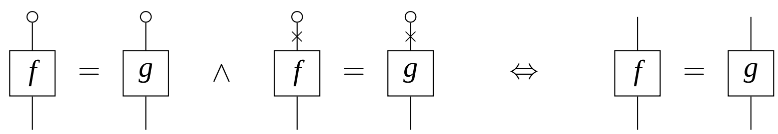
where we used distributivity and ignored the scalars; this is fine as the scalars in corollary 3.4 are cancellable for all the points we are considering.

4 Additive inverses

The last thing we need to actually produce a field of fractions is additive inverses. Suppose we have an involutive operation  that is a phase for :

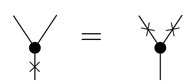


Suppose further that {, } forms a plugging set:

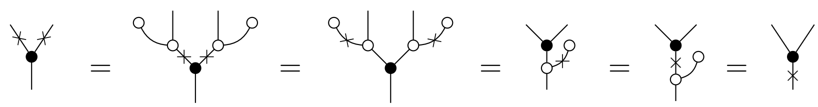


Then this will act as an additive inverse operation.

Lemma 4.1.

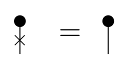


Proof.

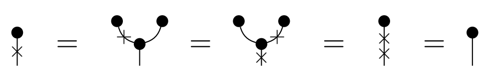


□

Lemma 4.2.

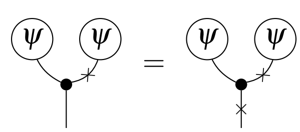


Proof.



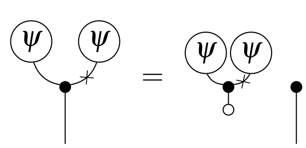
□

Lemma 4.3.



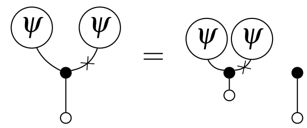
Proof. Follows immediately from Lemma 4.1 and the fact that  is an involution. □

Theorem 4.4. *The cross is additive inverse:*

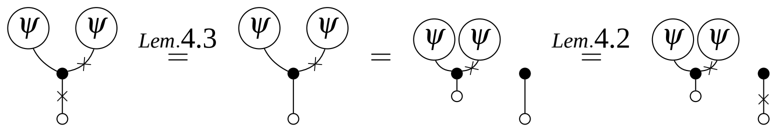


Proof. Proof by plugging: Recall that  $= 1_{\mathbf{I}}$.

a)



b)

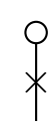


□

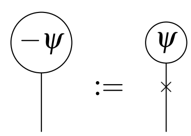
In the case of **FHilb**, this operation is the Pauli Z gate multiplied by -1:

 $= \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

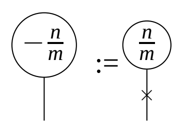
In this case, we have

 $= -\sqrt{2}|-\rangle = |1\rangle - |0\rangle$

We can now naturally define:



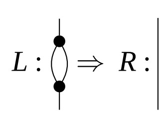
and, in particular,



Thus, we have reconstructed all of the axioms for the field of rational numbers. All of the expected identities involving  then follow from the field axioms.

5 !-boxes and automation

Graph rewriting is a computation process in which graphs are transformed by various *rewrite rules*. A rewrite rule can be thought of as a 'directed graphical equation'. For example, the "specialness" equation from section 2 could be expressed as a graph rewrite rule:

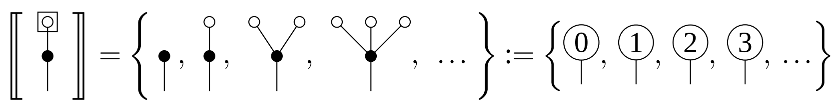


A graph rewrite rule $L \Rightarrow R$ can be applied to a graph G by identifying a *matching*, that is, a monomorphism $m : L \to G$. The image of L under m is then removed and replaced by R. This process is called *double pushout (DPO) graph rewriting*. A detailed description of how DPO graph rewriting can be performed on the graphs described in this paper is available in [11].

It is also useful to talk not only about ‘concrete’ graph rewrite rules, but also *pattern graph* rewrite rules, which can be used to express an infinite set of rewrite rules. We form pattern graphs using *!-boxes* (or ‘bang-boxes’). These boxes identify portions of the graph that can be replicated any number of times. More precisely, the set of concrete graphs represented by a pattern graph is the set of all graphs (containing no !-boxes) that can be obtained by performing any sequence of these four operations:

- `COPY`: copy a !-box and its incident edges
- `MERGE`: merge two !-boxes
- `DROP`: remove a !-box, leaving its contents
- `KILL`: remove a !-box and its contents

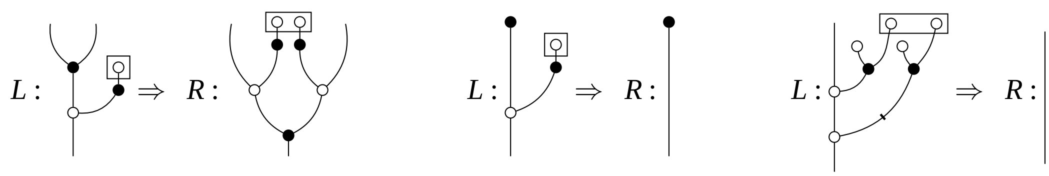
For example, the following pattern graph represents the encoding of a natural number given in section 3.2:



Note how not only the vertices are duplicated, but also all of the edges connected to those vertices.

A pattern graph rewrite rule is a pair of pattern graphs with the same inputs and outputs. Furthermore, there is a bijection between the !-boxes occurring on the LHS and the RHS. When one of the four operations is performed to a !-box on the LHS, the same is performed to its corresponding !-box on the RHS.

We can rewrite (the natural numbers versions of) equations δ_1, δ_2, and δ_3 as pattern graph rewrite rules.

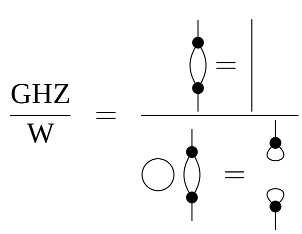


These equations only apply to encodings of the natural numbers, not for arbitrary inputs ψ. However, we showed in sections 3.2, 3.3, and 4 that even those weaker equations suffice to recover the usual identities for fraction arithmetic. Also note that the extra white vertices in δ_3' eliminate the case of $\frac{0}{0} \neq 1$.

So why bother expressing graphical identities as graph rewrite rules? Graph rewriting can be automated! `quantomatic` [10] is a automatic graph rewriting tool developed by two of the authors. It is specifically designed to work with the kinds of diagram described in this paper and to perform pattern graph rewriting. It remains to be seen what new insights can be obtained by adding the new graphical identities derived in this paper to `quantomatic`.

6 Closing Remarks

In previous work two of the authors showed that the main difference between the GHZ state and the W state, or more precisely, the induced GHZ structure and W structure, boils down to the value of the loop map of these CFAs:



In this paper, by focussing on the interaction of these two structures, we were able to establish a connection with the operations of basic arithmetic:

$$\frac{\mathrm{W}}{\mathrm{GHZ}} = \frac{+}{\times}$$

More specifically, the diagrammatic language of these structures was sufficient to encode the positive rational numbers (and, with a minor extension, the whole field of rational numbers).

In the process of highlighting this encoding, we identified a surprising fact. The distributive law governing the interaction of addition and multiplication in arithmetic also captures the interaction of the GHZ-structure and W-structure. Future work includes exploiting this interaction in the study of multipartite quantum entanglement, which brings us back to the initial motivation for crafting a compositional framework to reason about multipartite states.

References

[1] S. Abramsky & B. Coecke (2004): *A categorical semantics of quantum protocols*. In: *Proceedings of the 19th Annual IEEE Symposium of Logic in Computer Science*. IEEE Computer Science Press, pp. 415–425. Extended version: arXiv:0808.1023.

[2] M. Aguiar (2000): *A note on strongly separable algebras*. *Boletín de la Academia Nacional de Ciencias (Córdoba, Argentina)* 65, pp. 51–60.

[3] A. Carboni & R. F. C. Walters (1987): *Cartesian bicategories I*. *Journal of Pure and Applied Algebra* 49, pp. 11–32.

[4] B. Coecke (2009): *Quantum Picturalism*. *Contemporary Physics* 51, pp. 59–83. arXiv:0908.1787.

[5] B. Coecke & R. Duncan (2008): *Interacting quantum observables*. In: *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP)*, Lecture Notes in Computer Science. Extended version: arXiv:quant-ph/09064725.

[6] B. Coecke, B. Edwards & R. W. Spekkens (2011): *Phase groups and the origin of non-locality for qubits*. *Electronic Notes in Theoretical Computer Science* 270(2), pp. 15–36. arXiv:1003.5005.

[7] B. Coecke & A. Kissinger (2010): *The Compositional Structure of Multipartite Quantum Entanglement*. In: *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP)*, Lecture Notes in Computer Science. pp. 297–308. Extended version: arXiv:1002.2540.

[8] B. Coecke & D. Pavlovic (2007): *Quantum measurements without sums*. In: G. Chen, L. Kauffman & S. Lamonaco, editors: *Mathematics of Quantum Computing and Technology*. Taylor and Francis, pp. 567–604. arXiv:quant-ph/0608035.

[9] L. Dixon & R. Duncan (2009): *Graphical reasoning in compact closed categories for quantum computation*. *Annals of Mathematics and Artificial Intelligence* 51, pp. 23–42.

[10] L. Dixon, R. Duncan, A. Merry & A. Kissinger (2011): `quantomatic` *software*. Available from http://dream.inf.ed.ac.uk/projects/quantomatic/.

[11] L. Dixon & A. Kissinger (2011): *Open graphs and monoidal theories*. arXiv:1011.4114.

[12] R. Duncan (2006). *Types for Quantum Computation*. DPhil Thesis, Oxford University.

[13] R. Duncan & S. Perdrix (2010): *Rewriting measurement-based quantum computations with generalised flow*. In: *Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP)*, Lecture Notes in Computer Science. pp. 285–296.

[14] W. Dür, G. Vidal & J. I. Cirac (2000): *Three qubits can be entangled in two inequivalent ways*. *Phys. Rev. A* 62(062314).

[15] M. Herrmann (2010). *Models of Multipartite Entanglement*. MSc Thesis, Oxford University.

[16] A. Joyal & R. Street (1991): *The geometry of tensor calculus I*. *Advances in Mathematics* 88, pp. 55–112.

[17] G. M. Kelly & M. L. Laplaza (1980): *Coherence for compact closed categories*. *Journal of Pure and Applied Algebra* 19, pp. 193–213.

[18] S. Lack (2004): *Composing PROPs*. *Theory and Applications of Categories* 13, pp. 147–163.

[19] R. Penrose (1971): *Applications of negative dimensional tensors*. In: *Combinatorial Mathematics and its Applications*. Academic Press, pp. 221–244.

[20] P. Selinger (2011): *A survey of graphical languages for monoidal categories*. In: B. Coecke, editor: *New Structures for Physics*, Lecture Notes in Physics. Springer-Verlag, pp. 275–337. arXiv:0908.3347.